

October 2002

# INFORMATION SECURITY

## Vulnerability Scanning Requirements for GISRA Under OMB M-02-09

Reporting Instructions for the  
Government Information Security  
Reform Act (GISRA) and Updated  
Guidance on Security Plans of  
Action and Milestones

Plus A Case Study of Effective Agency-  
Wide Vulnerability Scanning and  
Remediation at the National Aeronautics  
and Space Administration (NASA).

---

October 2, 2002

On March 6, 2002, Robert Dacey, Director of Information Security Issues at the U.S. General Accounting Office, testified before the Subcommittee on Government Efficiency, Financial Management and Intergovernmental Relations, Committee on Government Reform, of the House of Representatives. He recommended that the U.S. Office of Management and Budget provide additional guidance to federal agencies on carrying out their responsibilities under the Government Information Security Reform provisions of the National Defense Authorization Act for 2001 (commonly known as GISRA).

In his testimony, Mr. Dacey told the members of Congress that federal security controls had not been adequately tested and evaluated, and remedial actions may not be adequate. He also testified that "more specific guidance [from OMB] to agencies on the controls they need to implement [to improve security] could help ensure adequate protection", and asserted that specific mandatory standards for various risk levels are important elements of a security program. He added that the National Institute of Standards and Technology, with the assistance of the National Security Agency, is responsible for establishing related standards. (<http://www.gao.gov/new.items/d02470t.pdf>)

In a subsequent letter, delivered to the Subcommittee on May 2, 2002, Mr. Dacey reported that OMB needed to define which systems must be reviewed and define the security controls that must be tested. (<http://www.gao.gov/new.items/d02407.pdf>)

---

**OMB Acts to  
Clarify  
GISRA  
Guidance**

Recognizing the need for better guidance, on July 2, 2002, OMB issued Memorandum 02-09, *Reporting Instructions for the Government Information Security Reform Act* and Updated Guidance on Security Plans of Action and Milestones. (<http://www.whitehouse.gov/omb/memoranda/m02-09.pdf>)

In this Memorandum, OMB laid out the following requirements that agencies must meet:

"Use the National Institute of Standards and Technology (NIST) Self-Assessment Guide (Special Publication 800-26, 'Security Self-Assessment Guide for Information Technology Systems.')

to review their systems ...unless they and the IG confirm... that any agency-developed methodology captures all elements of the NIST guide," and provide

---

quarterly updates of progress for the President's Management Scorecard.

Two sections of the NIST Self-Assessment Guide, Special Publication 800-26 (<http://csrc.nist.gov/publications/nistpubs/800-26/sp800-26.pdf>), define the specific requirement for regular periodic testing of systems (scanning) for vulnerabilities:

- (1) Section 10.3.1 requires that "systems [be] reviewed periodically to identify and, when possible, eliminate unnecessary services (e.g. FTP. HTTP. Mainframe supervisory calls, etc.)."
- (2) Section 10.3.2 requires that the "systems [are] periodically reviewed for known vulnerabilities, and patches promptly installed."

These two components of the requirement -- periodic review for known vulnerabilities and prompt installation of patches -- are indispensable technical actions for effective security management on Internet-connected systems. Most agencies did **not** undertake comprehensive periodic reviews of these critical aspects of their systems last year. At least they did not report the results of these reviews to OMB. Under the new guidance, organizations that fail to scan all systems regularly and report on progress in eliminating the most critical vulnerabilities are clearly in violation. But there is an even more important reason to implement a program for quarterly, agency-wide vulnerability scanning and remediation: It works! NASA's experience proves that comprehensive, agency-wide programs actually turn the tide against the hackers.

---

**NASA  
Provides a  
Model for  
Effective  
Practice**

The National Aeronautics and Space Administration has demonstrated the efficacy of a broad-based, targeted vulnerability scanning and remediation program -- for more than 80,000 computers in ten major facilities.

In the summer of 1999, the NASA CIO identified approximately 50 of the most serious vulnerabilities whose presence on a computer could be verified by network scanning tools. The CIO purchased and deployed to all Centers a standard suite of network scanning tools, and trained field security staff how to use them. The CIO required that all organizations report the scanning results to the CIO quarterly

---

Starting in Fiscal Year 2000, each quarter all network-connected NASA computers were scanned for the listed vulnerabilities, and system owners were informed of their vulnerabilities and how to eliminate them. Scanning data was transmitted quarterly to the CIO. The CIO set a target that each Center would achieve a ratio of fewer than one listed vulnerability per four computers scanned (or 0.25 vulnerabilities per system scanned.) Initially the observed ratio exceeded one, but by the end of FY00 it had dropped to 0.16, with over 80,000 systems scanned. For FY01 the target ratio was reduced to 0.01, and by the end of FY01 the ratio stood at 0.0068. An updated list of serious vulnerabilities was introduced in FY01 to replace the first list, with an initial target ratio of 0.25, and by the end of FY01 the ratio for that list stood at 0.097.

Healthy competition developed among Centers to reduce the ratio, and computer owners became more aware of and more involved with fixing vulnerabilities on their systems. For FY02, NASA further refined the process by updating the list each quarter to catch emergent serious vulnerabilities, keeping the same target ratio of 0.25. In addition, NASA has required emergency scanning, remediation and reporting for a few very fast-developing exploits.

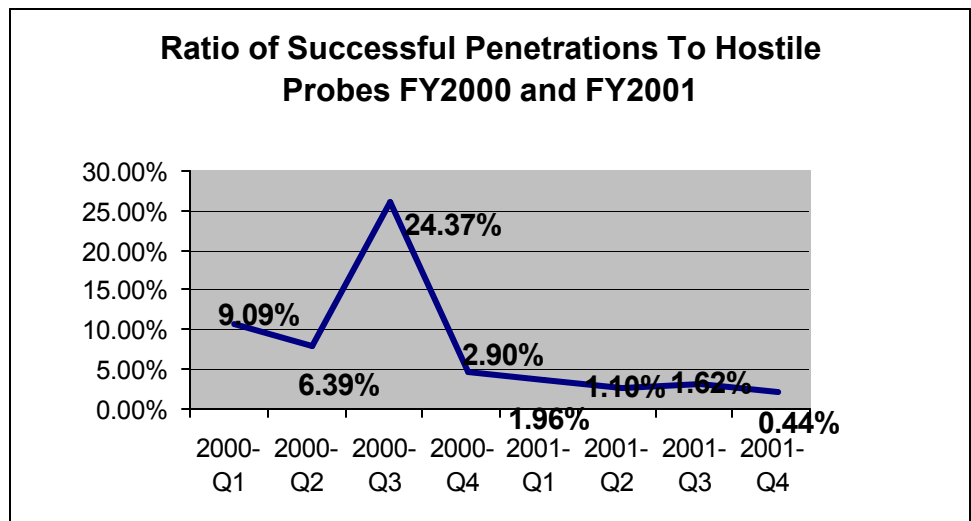
The cost of this project is almost entirely in labor. Each of the ten NASA Centers devotes a substantial part of one or two staff (depending on Center size) to scanning, reporting, and monitoring, and individual system administrators assist them. Total cost is therefore between \$2 million and \$3 million per year, or about \$30 per computer per year.

NASA focused on the most important vulnerabilities, rather than all possible vulnerabilities, because NASA data, like that of other organizations, showed that a few vulnerabilities were responsible for most of our compromises. This made the problem of reducing vulnerabilities more manageable, and NASA security staff became skilled at using scanning tools. Because the agency standardized on the scanning tools and the vulnerabilities to be scanned, results were comparable among Centers. System owners became more aware of system vulnerabilities and the importance of fixing them. Quarterly metrics showed where they were making progress and let the CIO focus on weak areas. Regular practice in scanning for and fixing vulnerabilities made NASA more adept at dealing with fast developing exploits.

---

The number of system compromises has been reduced, even though attacks have increased markedly. Focusing attention on the most important vulnerabilities has kept the cost of fixing vulnerabilities lower compared with trying to fix all vulnerabilities, and has helped to maintain user support for the security program.

The figure above shows the ratio of successful penetrations to hostile probes, which are attempted attacks. At the first quarter of FY00, this ratio stood at 0.09, and after a very bad third quarter of FY00, it has continued to drop. At the end of FY01 the ratio stood at 0.004, or almost three times better than when NASA began its vulnerability reduction program. As a result NASA has been spared the cost of cleaning up additional compromises and consequences of disrupted services.



In addition, NASA appears to have fewer problems with fast-spreading exploits than they used to, because through the scanning program they have often eliminated the vulnerability before the exploit spreads. Because they are set up to rapidly scan for vulnerabilities and fix them, at the first sign of an emergency exploit warning, they can quickly identify and fix the vulnerability.

---

---

Of course, NASA has also improved other parts of its information security program, including better training, better attention to security plans, better security architecture, and better intrusion detection, so it is hard to attribute all of the improvement to vulnerability reduction. Nonetheless, the Agency believes targeted vulnerability scanning and elimination has been an important contributor to the improvement.

---

### **Draft National Strategy for Securing Cyber Space Targets Vulnerability Scanning**

In President Bush's Draft National Strategy for Securing Cyber Space, implementing programs for discovery and remediation of vulnerabilities is repeatedly emphasized. The strategy calls regular monitoring and remediation one of the "best practices", and strongly recommends that federal agencies use automated tools for continuously auditing the security posture of information technology systems.  
(<http://www.whitehouse.gov/pcipb/cyberstrategy-draft.pdf>)

Specifically, for Federal Agencies, the Draft National Strategy asks agencies to "Continuously Assess Threats and Vulnerabilities and Understand the Risks They Pose to Agency Operations and Assets. Commercial automated auditing and reporting mechanisms are now available to validate the effectiveness of security controls across a system and are **essential** [emphasis added] to continuously understand risks to those systems. Some, but not all, civilian agencies have taken steps to increase the use of these automated tools. More agencies need to do so. Therefore, the Federal government will drive the greatly expanded use of effective automated tools to ... conduct periodic vulnerability assessments, ... and continuously audit the security posture of information technology systems."

---

### **Questions**

If you have any questions concerning this report please email me at [paller@sans.org](mailto:paller@sans.org)